WHAT IS CLAIMED IS:

1. A method of defining the security vulnerability of a computer system, comprising:

specifying an attack representing a recognized vulnerability of the computer system;

specifying at least one attribute of the specified attack;

specifying at least one policy definition with respect to detecting the vulnerability of the specified attack; and

specifying a remedy for the specified vulnerability.

2. The method, as set forth in claim 1, further comprising specifying at least one attribute of the specified policy definition.

3. The method, as set forth in claim 1, further comprising specifying a computing platform of the computer system.

4. The method, as set forth in claim 1, further comprising:

specifying a security category of the specified attack; and

specifying at least one policy group with respect to the specified security category.

5. The method, as set forth in claim 1, further comprising specifying a vulnerability scanner executing on the computer system.

6. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying an identification of the severity associated with a breach of the computer system by the attack.

7. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying a description of the attack.

8. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying an explanation of why the specified attack is important.

9. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying how information is to be reported to a user with respect to the specified attack.

10. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying a source of a remedy operable to fix the specified vulnerability.

11. The method, as set forth in claim 1, wherein specifying at least one attribute of the specified attack comprises specifying information to enable a manual remedy of the specified vulnerability.

12. A method of defining a security vulnerability condition of a system, comprising:

specifying a name of a vulnerability associated with the system;

specifying at least one attribute of the specified vulnerability;

specifying a remedy for the vulnerability according to the specified computing platform;

specifying a policy definition with respect to the specified vulnerability; and

specifying at least one attribute of the specified policy definition.

13. The method, as set forth in claim 12, further comprising specifying a computing platform of the system.

14. The method, as set forth in claim 12, further comprising:

specifying a security category of the specified vulnerability; and

specifying at least one policy group with respect to the specified security category.

15. The method, as set forth in claim 12, further comprising specifying a vulnerability scanner executing on the system.

16. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified vulnerability comprises specifying an identification of the severity associated with a breach of the specified vulnerability.

17. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified vulnerability comprises specifying an explanation of why the specified vulnerability is important.

18. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified vulnerability comprises specifying how information is to be reported to a user in response to detecting the specified vulnerability.

19. The method, as set forth in claim 12, wherein specifying at least one attribute of the specified vulnerability comprises specifying an application operable to respond to a detection of the specified vulnerability.

20. A system of defining security vulnerabilities of a computer system, comprising:

a vulnerability description file containing a definition of at least one vulnerability, a definition of at least one policy item for the vulnerability;

an interpreter operable to parse the at least one vulnerability definition and at least one policy item definition in the vulnerability description file and organize the parsed definitions pursuant to a predetermined format; and

a data storage operable to store the parsed and organized at least one vulnerability and at least one policy item definition, wherein the data storage is accessible by at least one vulnerability scanner application.

21. The system, as set forth in claim 20, wherein the data storage is a relational database having a plurality of tables.

22. The system, as set forth in claim 20, wherein the vulnerability description file further comprises a definition of a vulnerability scanner application.

23. The system, as set forth in claim 20, wherein the vulnerability description file further comprises a definition of a security category providing a grouping of the at least one vulnerability, and a definition of a policy group providing a grouping of the at least one policy item.

24. The system, as set forth in claim 20, wherein the vulnerability description file further comprises a definition of at least one attribute of the at least one vulnerability.

25. The system, as set forth in claim 20, wherein the vulnerability description file further comprises an identification of the severity of risk associated with the at least one vulnerability.

26. The system, as set forth in claim 20, wherein the vulnerability description file further comprises a definition of how information is to be displayed to a user with respect to the at least one vulnerability.

27. The system, as set forth in claim 20, wherein the vulnerability description file further comprises a definition of an application operable to respond to detecting the at least one vulnerability.